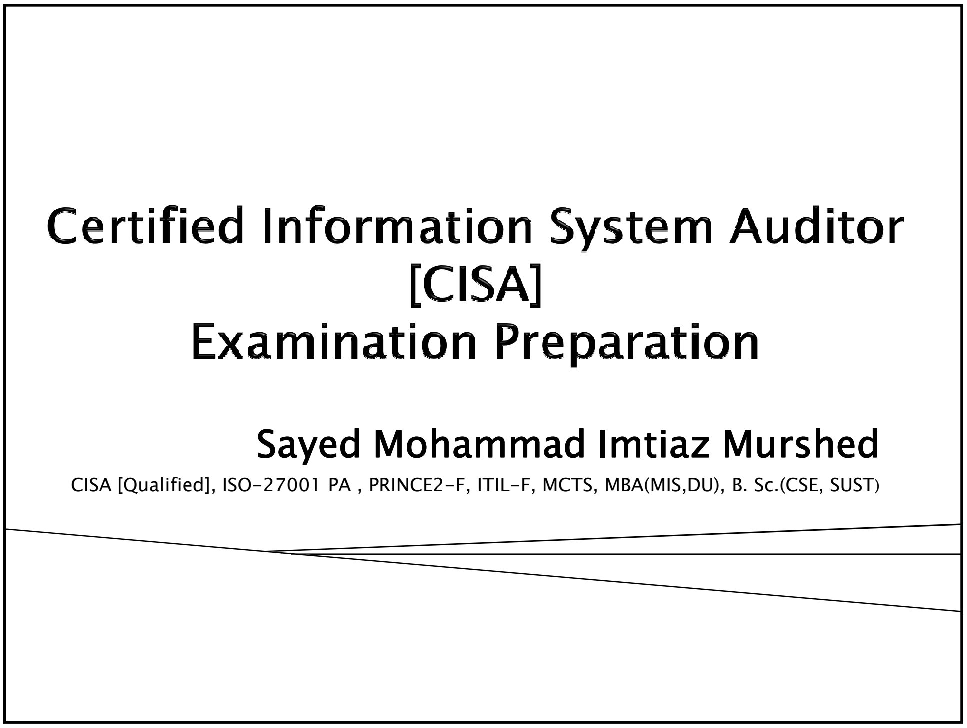
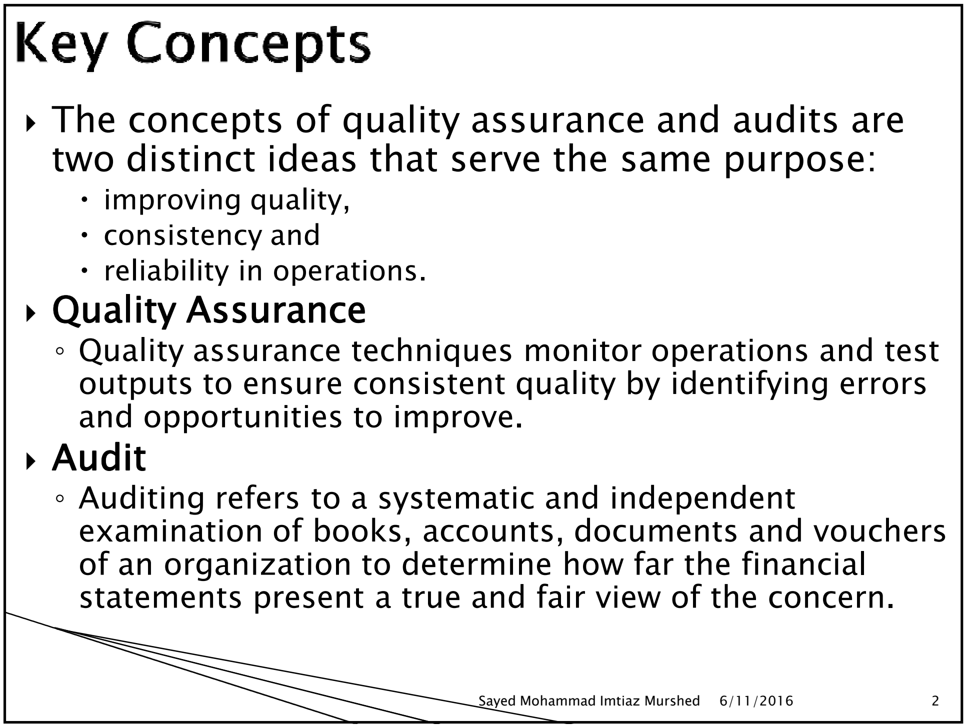


Certified Information System Auditor [CISA] Examination Preparation

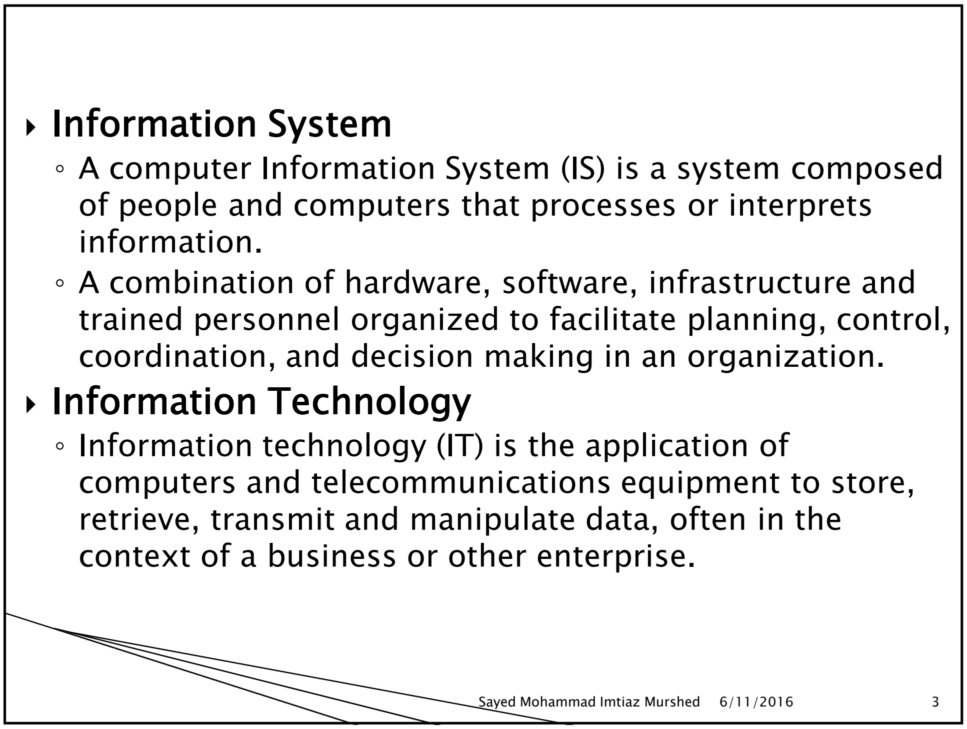
Sayed Mohammad Imtiaz Murshed

CISA [Qualified], ISO-27001 PA , PRINCE2-F, ITIL-F, MCTS, MBA(MIS,DU), B. Sc.(CSE, SUST)

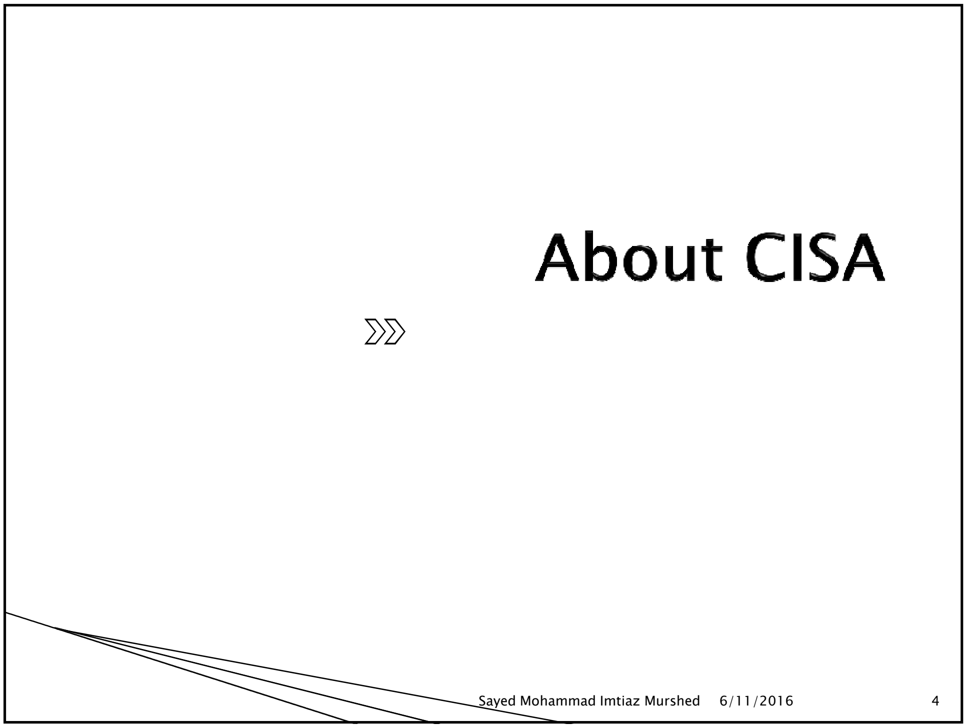


Key Concepts

- The concepts of quality assurance and audits are two distinct ideas that serve the same purpose:
  - improving quality,
  - consistency and
  - reliability in operations.
- Quality Assurance
  - Quality assurance techniques monitor operations and test outputs to ensure consistent quality by identifying errors and opportunities to improve.
- Audit
  - Auditing refers to a systematic and independent examination of books, accounts, documents and vouchers of an organization to determine how far the financial statements present a true and fair view of the concern.



- **Information System**
  - A computer Information System (IS) is a system composed of people and computers that processes or interprets information.
  - A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.
- **Information Technology**
  - Information technology (IT) is the application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.



About CISA

About ISACA

- Independent, nonprofit, global association
- Engages in
  - development,
  - adoption and
  - use

  of globally accepted, industry-leading knowledge and practices for information systems.
- ISACA got its start in 1967
- Previously known as the Information Systems Audit and Control Association
- ISACA now goes by its acronym only
- ISACA serves 140,000 professionals in 180 countries

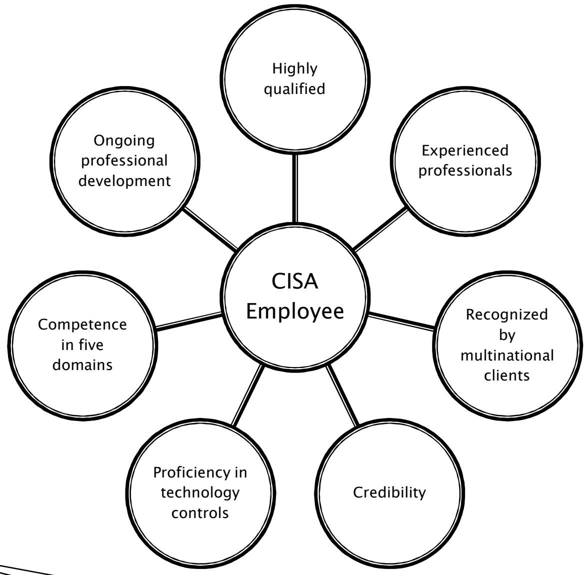
ISACA certifications

CISA
Certified Information Systems Auditor
An ISACA Certification
CISM
Certified Information Security Manager
An ISACA Certification
CGEIT
Certified in the Governance of Enterprise IT
An ISACA Certification
CRISC
Certified in Risk and Information Systems Control
An ISACA Certification
CSX
CYBERSECURITY NEXUS

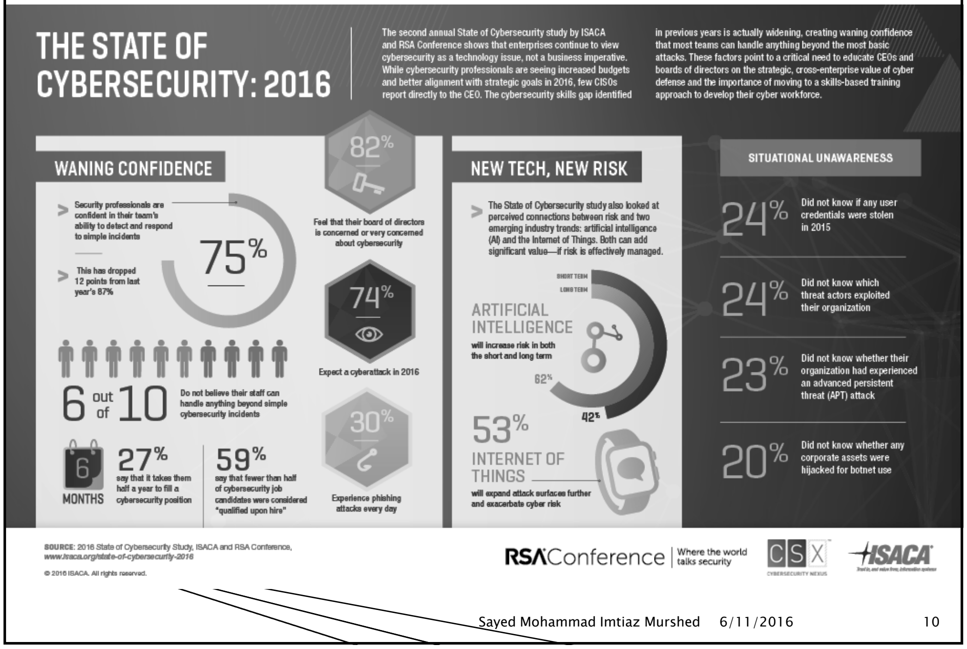
CISA – at a glance

- Globally recognized certification in the field of audit, control and security of information systems
- CISA certification has been earned by more than 109,000 professionals since inception
- CISA is designed for:
  - IS/IT Auditors
  - IS/IT Consultants
  - CIO
  - IS/IT Audit Managers
  - Security Professionals
  - Non-IT Auditors

Why Employers Hire CISAs


Highly qualified
Ongoing professional development
Experienced professionals
CISA Employee
Competence in five domains
Recognized by multinational clients
Proficiency in technology controls
Credibility

How certificate helps to build career



THE STATE OF CYBERSECURITY: 2016

The second annual State of Cybersecurity study by ISACA and RSA Conference shows that enterprises continue to view cybersecurity as a technology issue, not a business imperative. While cybersecurity professionals are seeing increased budgets and better alignment with strategic goals in 2016, few CISOs report directly to the CEO. The cybersecurity skills gap identified in previous years is actually widening, creating waning confidence that most teams can handle anything beyond the most basic attacks. These factors point to a critical need to educate CEOs and boards of directors on the strategic, cross-enterprise value of cyber defense and the importance of moving to a skills-based training approach to develop their cyber workforce.

WANING CONFIDENCE

75% — Security professionals are confident in their team's ability to detect and respond to simple incidents

This has dropped 12 points from last year's 87%

6 out of 10 — Do not believe their staff can handle anything beyond simple cybersecurity incidents

6 MONTHS — 27% say that it takes them half a year to fill a cybersecurity position

59% say that fewer than half of cybersecurity job candidates were considered "qualified upon hire"

82% — Feel that their board of directors is concerned or very concerned about cybersecurity

74% — Expect a cyberattack in 2016

30% — Experience phishing attacks every day

NEW TECH, NEW RISK

The State of Cybersecurity study also looked at perceived connections between risk and two emerging industry trends: artificial intelligence (AI) and the Internet of Things. Both can add significant value—if risk is effectively managed.

ARTIFICIAL INTELLIGENCE will increase risk in both the short and long term

53% INTERNET OF THINGS will expand attack surfaces further and exacerbate cyber risk

SITUATIONAL UNAWARENESS

24% Did not know if any user credentials were stolen in 2015

24% Did not know which threat actors exploited their organization

23% Did not know whether their organization had experienced an advanced persistent threat (APT) attack

20% Did not know whether any corporate assets were hijacked for botnet use

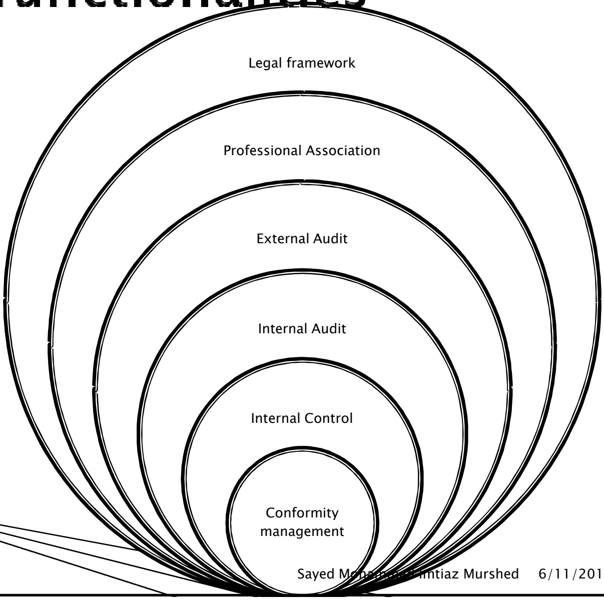
SOURCE: 2016 State of Cybersecurity Study, ISACA and RSA Conference, *www.isaca.org/state-of-cybersecurity-2016*

RSAConference | Where the world talks security

CSX CYBERSECURITY NEXUS

ISACA

Control Environment and need of Audit functionalities



Legal framework

Professional Association

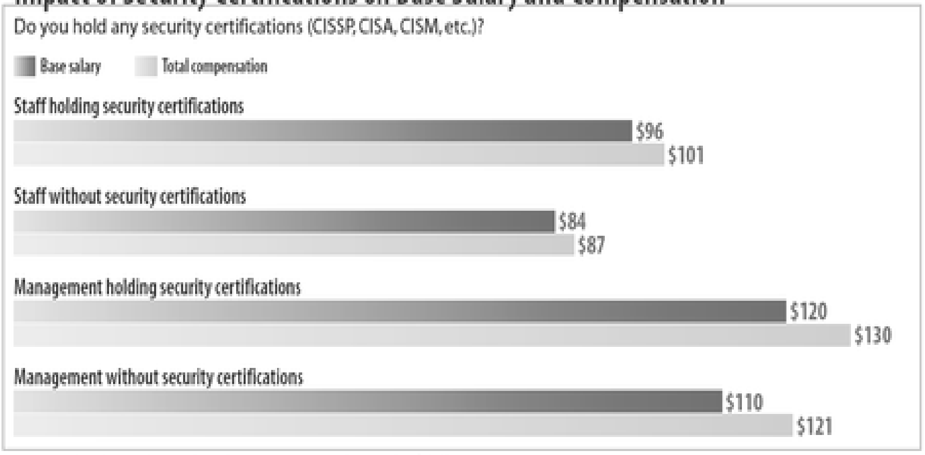
External Audit

Internal Audit

Internal Control

Conformity management

Impact of Security Certifications on Base Salary and Compensation

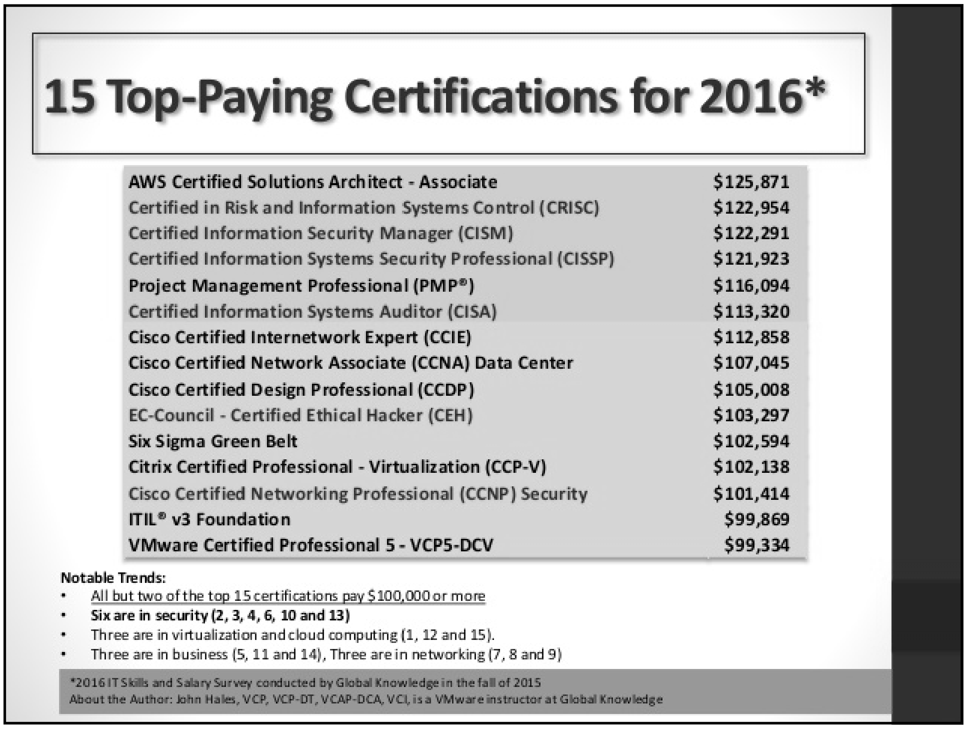


Do you hold any security certifications (CISSP, CISA, CISM, etc.)?

Note: Median base salary and total compensation in thousands of dollars R6460413-SEC/56

Base: 390 staff and 292 managers

Data: *InformationWeek* 2013 U.S. IT Salary Survey of 682 IT security professionals, January 2013



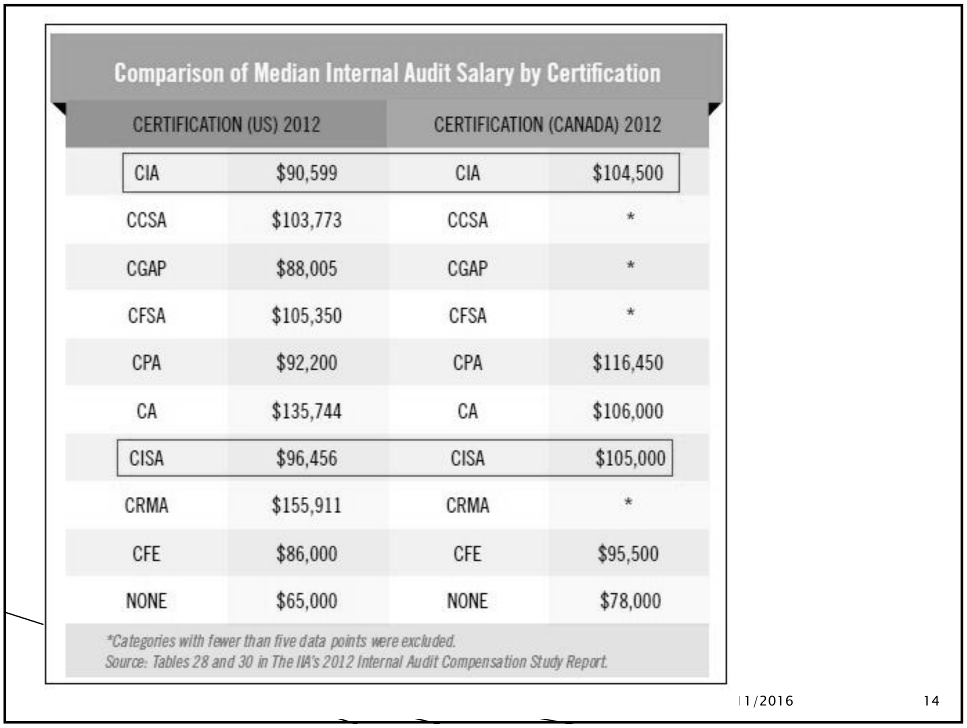
15 Top-Paying Certifications for 2016*

AWS Certified Solutions Architect - Associate	**$125,871**
Certified in Risk and Information Systems Control (CRISC)	**$122,954**
Certified Information Security Manager (CISM)	**$122,291**
Certified Information Systems Security Professional (CISSP)	**$121,923**
Project Management Professional (PMP®)	**$116,094**
Certified Information Systems Auditor (CISA)	**$113,320**
Cisco Certified Internetwork Expert (CCIE)	**$112,858**
Cisco Certified Network Associate (CCNA) Data Center	**$107,045**
Cisco Certified Design Professional (CCDP)	**$105,008**
EC-Council - Certified Ethical Hacker (CEH)	**$103,297**
Six Sigma Green Belt	**$102,594**
Citrix Certified Professional - Virtualization (CCP-V)	**$102,138**
Cisco Certified Networking Professional (CCNP) Security	**$101,414**
ITIL® v3 Foundation	**$99,869**
VMware Certified Professional 5 - VCP5-DCV	**$99,334**

Notable Trends:

- All but two of the top 15 certifications pay $100,000 or more
- **Six are in security (2, 3, 4, 6, 10 and 13)**
- Three are in virtualization and cloud computing (1, 12 and 15).
- Three are in business (5, 11 and 14), Three are in networking (7, 8 and 9)

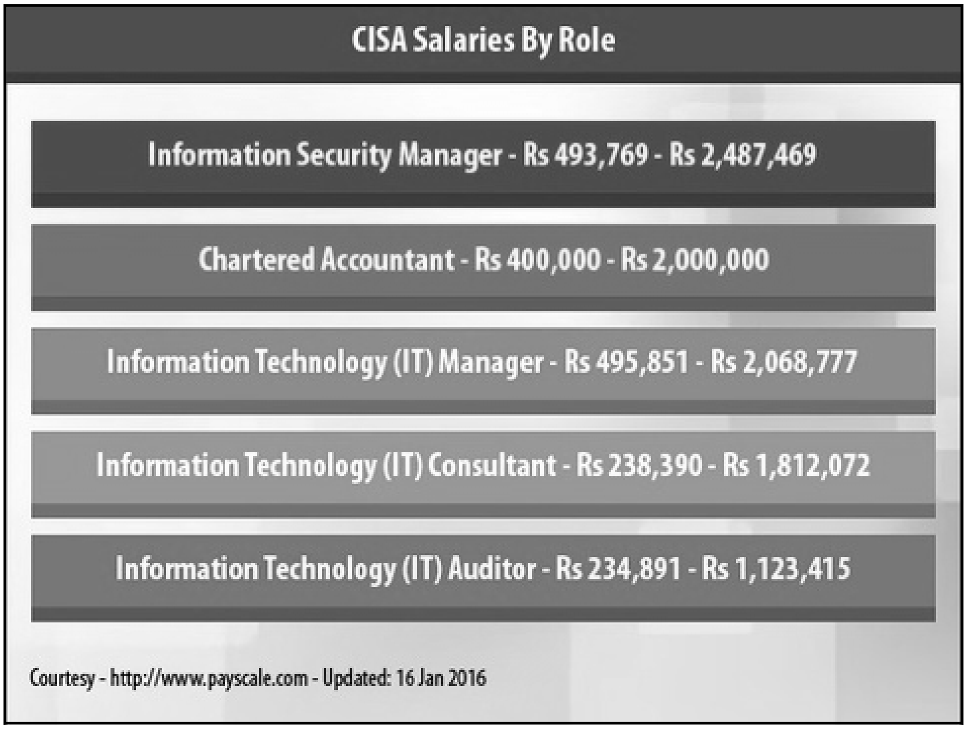
*2016 IT Skills and Salary Survey conducted by Global Knowledge in the fall of 2015
About the Author: John Hales, VCP, VCP-DT, VCAP-DCA, VCI, is a VMware instructor at Global Knowledge



Comparison of Median Internal Audit Salary by Certification

CERTIFICATION (US) 2012		CERTIFICATION (CANADA) 2012	
CIA	$90,599	CIA	$104,500
CCSA	$103,773	CCSA	*
CGAP	$88,005	CGAP	*
CFSA	$105,350	CFSA	*
CPA	$92,200	CPA	$116,450
CA	$135,744	CA	$106,000
CISA	$96,456	CISA	$105,000
CRMA	$155,911	CRMA	*
CFE	$86,000	CFE	$95,500
NONE	$65,000	NONE	$78,000

**Categories with fewer than five data points were excluded.*
Source: Tables 28 and 30 in The IIA's 2012 Internal Audit Compensation Study Report.



CISA Salaries By Role

Information Security Manager - Rs 493,769 - Rs 2,487,469

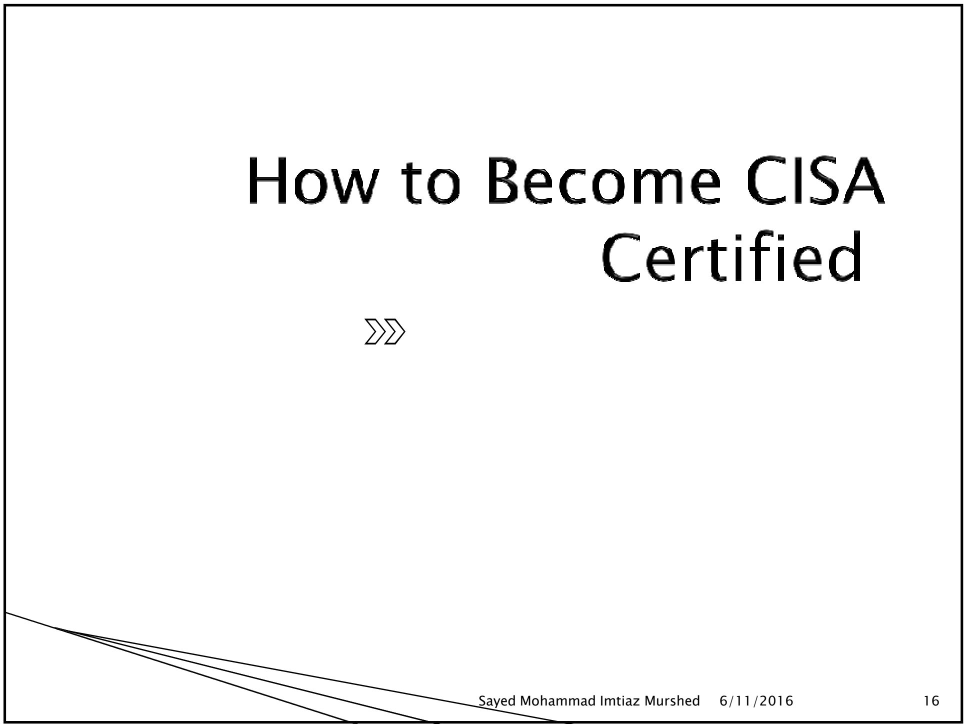
Chartered Accountant - Rs 400,000 - Rs 2,000,000

Information Technology (IT) Manager - Rs 495,851 - Rs 2,068,777

Information Technology (IT) Consultant - Rs 238,390 - Rs 1,812,072

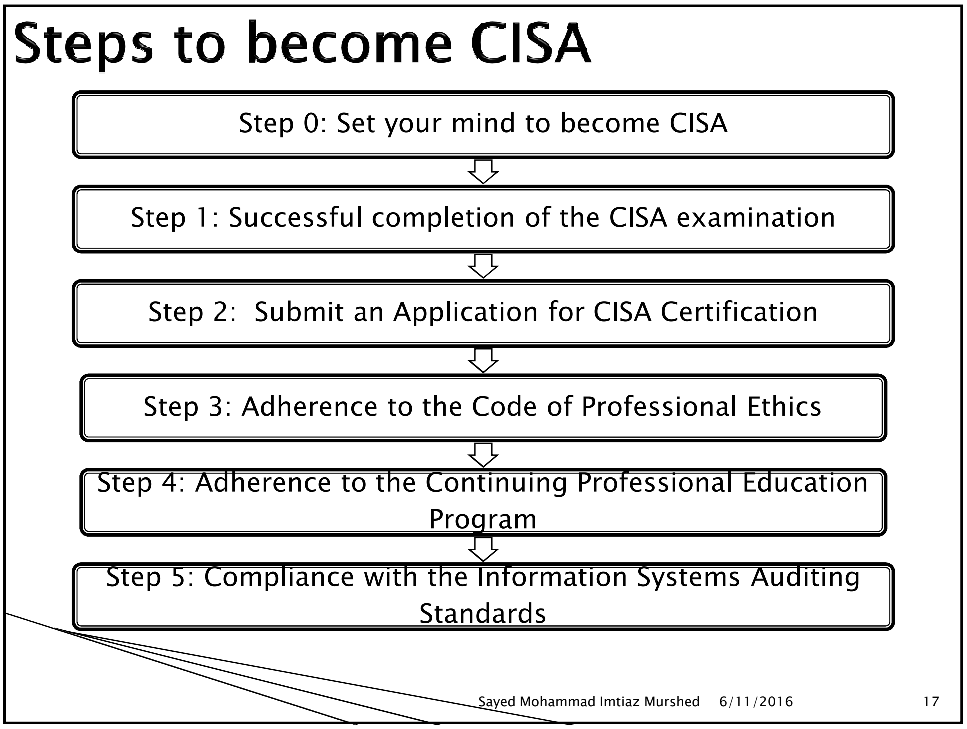
Information Technology (IT) Auditor - Rs 234,891 - Rs 1,123,415

Courtesy - http://www.payscale.com - Updated: 16 Jan 2016



How to Become CISA Certified

Sayed Mohammad Imtiaz Murshed 6/11/2016 16



Steps to become CISA

Step 0: Set your mind to become CISA

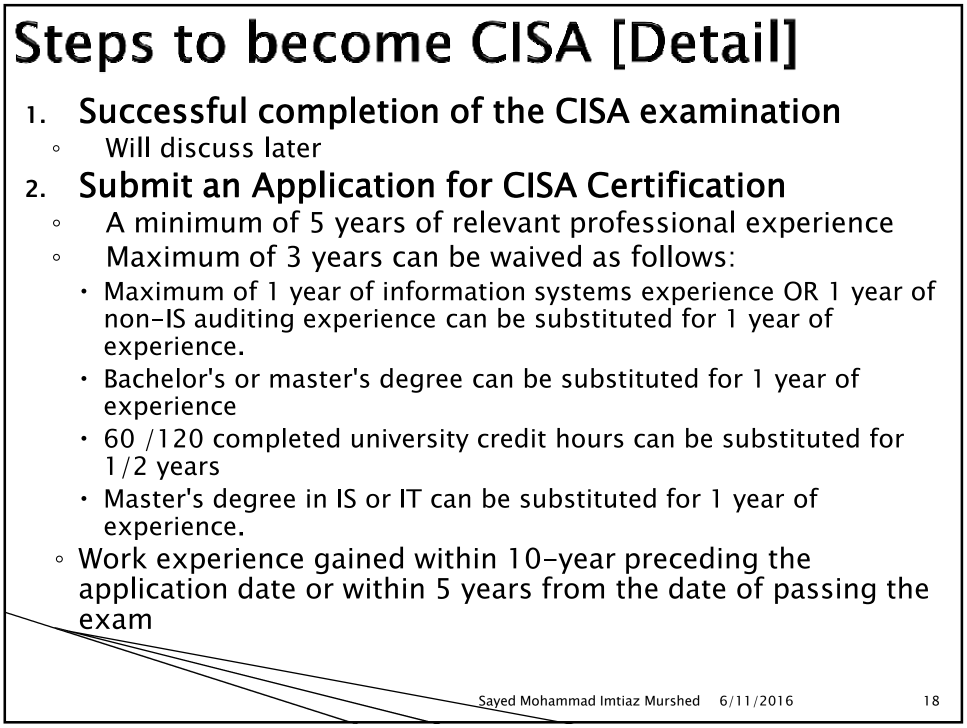
Step 1: Successful completion of the CISA examination

Step 2: Submit an Application for CISA Certification

Step 3: Adherence to the Code of Professional Ethics

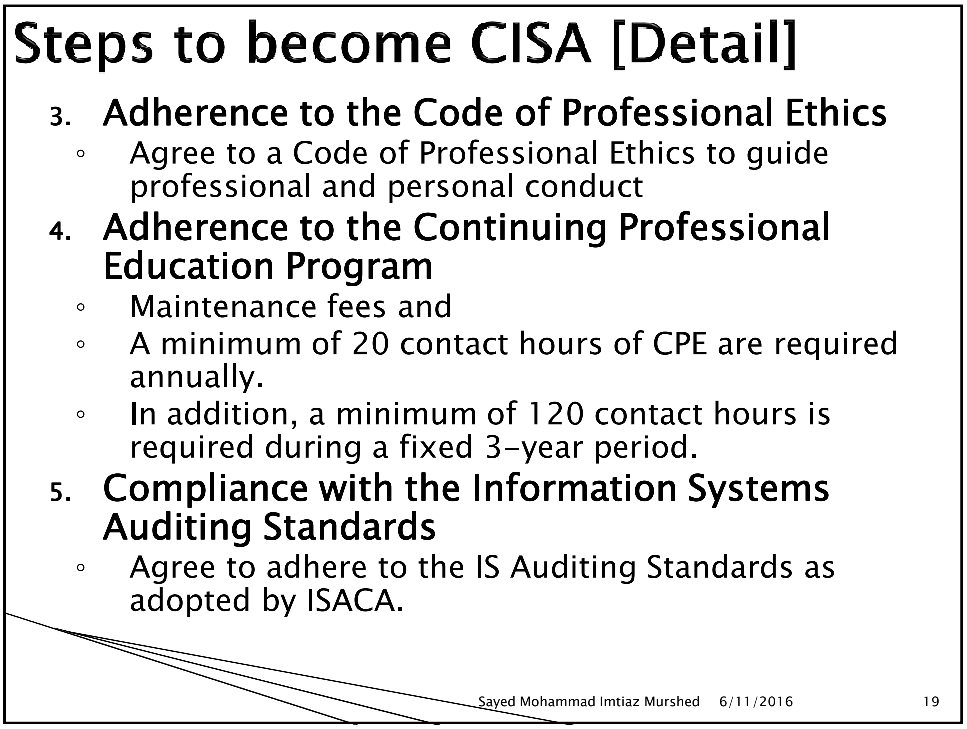
Step 4: Adherence to the Continuing Professional Education Program

Step 5: Compliance with the Information Systems Auditing Standards



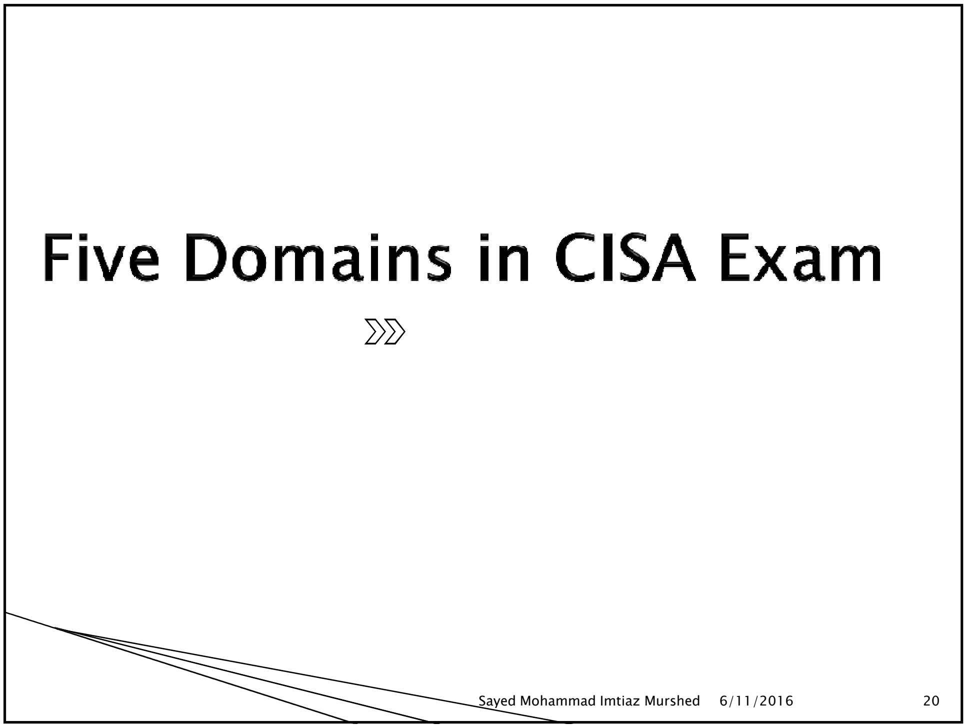
Steps to become CISA [Detail]

1. **Successful completion of the CISA examination**
   - Will discuss later
2. **Submit an Application for CISA Certification**
   - A minimum of 5 years of relevant professional experience
   - Maximum of 3 years can be waived as follows:
     - Maximum of 1 year of information systems experience OR 1 year of non-IS auditing experience can be substituted for 1 year of experience.
     - Bachelor's or master's degree can be substituted for 1 year of experience
     - 60 /120 completed university credit hours can be substituted for 1/2 years
     - Master's degree in IS or IT can be substituted for 1 year of experience.
   - Work experience gained within 10-year preceding the application date or within 5 years from the date of passing the exam

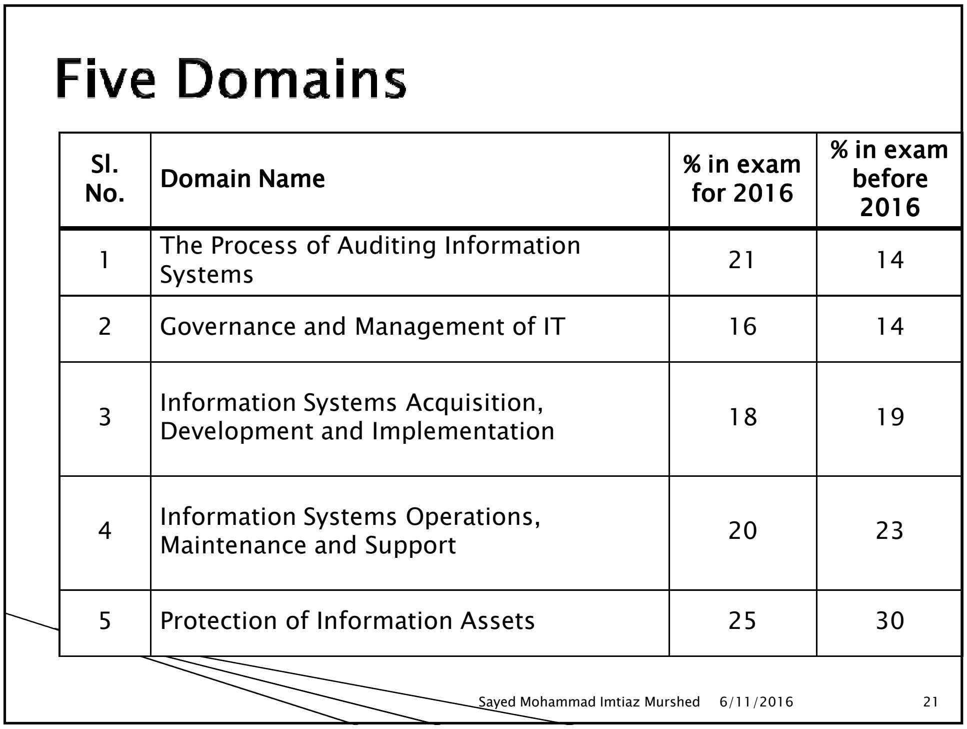


Steps to become CISA [Detail]

3. **Adherence to the Code of Professional Ethics**
   - Agree to a Code of Professional Ethics to guide professional and personal conduct
4. **Adherence to the Continuing Professional Education Program**
   - Maintenance fees and
   - A minimum of 20 contact hours of CPE are required annually.
   - In addition, a minimum of 120 contact hours is required during a fixed 3-year period.
5. **Compliance with the Information Systems Auditing Standards**
   - Agree to adhere to the IS Auditing Standards as adopted by ISACA.

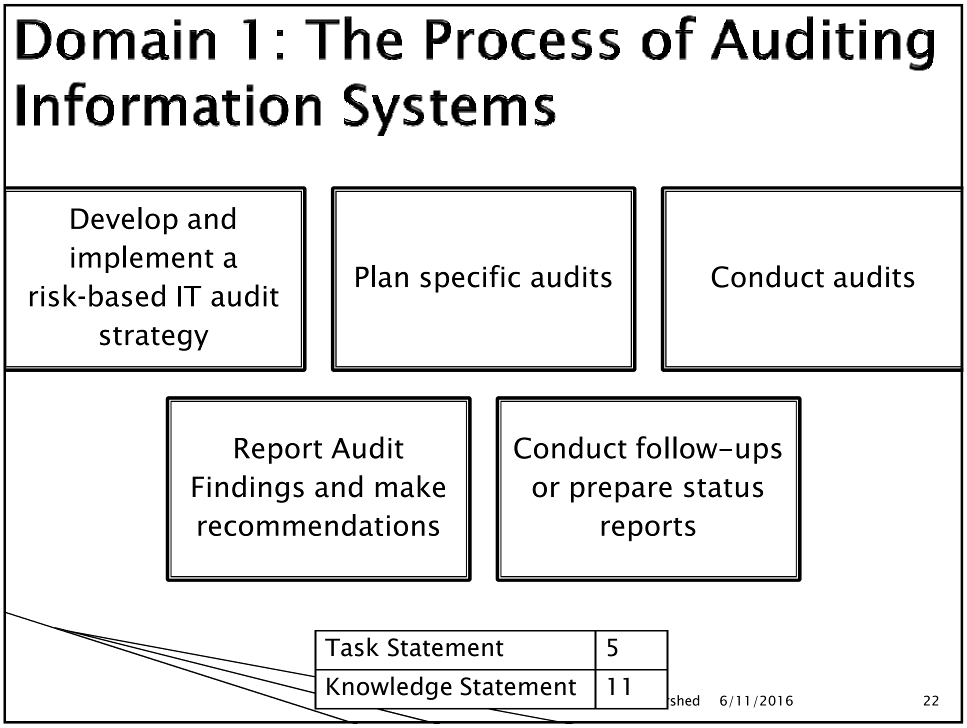


Five Domains in CISA Exam



Five Domains

Sl. No.	Domain Name	% in exam for 2016	% in exam before 2016
1	The Process of Auditing Information Systems	21	14
2	Governance and Management of IT	16	14
3	Information Systems Acquisition, Development and Implementation	18	19
4	Information Systems Operations, Maintenance and Support	20	23
5	Protection of Information Assets	25	30



Domain 1: The Process of Auditing Information Systems

Develop and implement a risk-based IT audit strategy

Plan specific audits

Conduct audits

Report Audit Findings and make recommendations

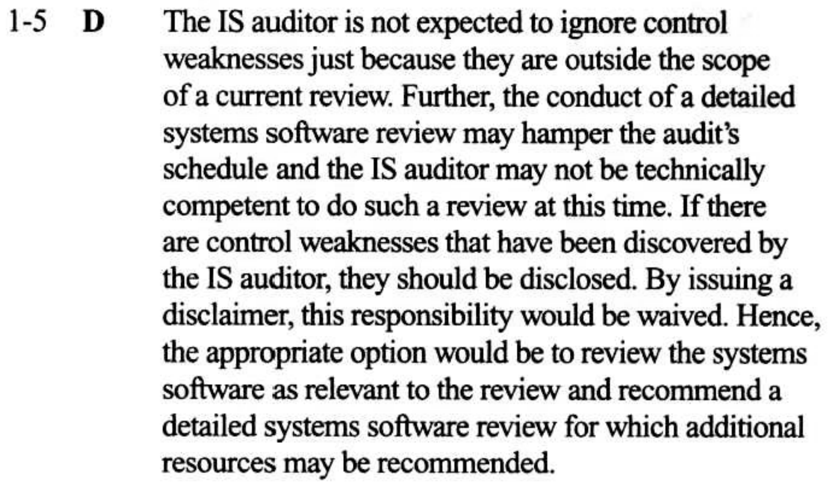
Conduct follow-ups or prepare status reports

Task Statement	5
Knowledge Statement	11

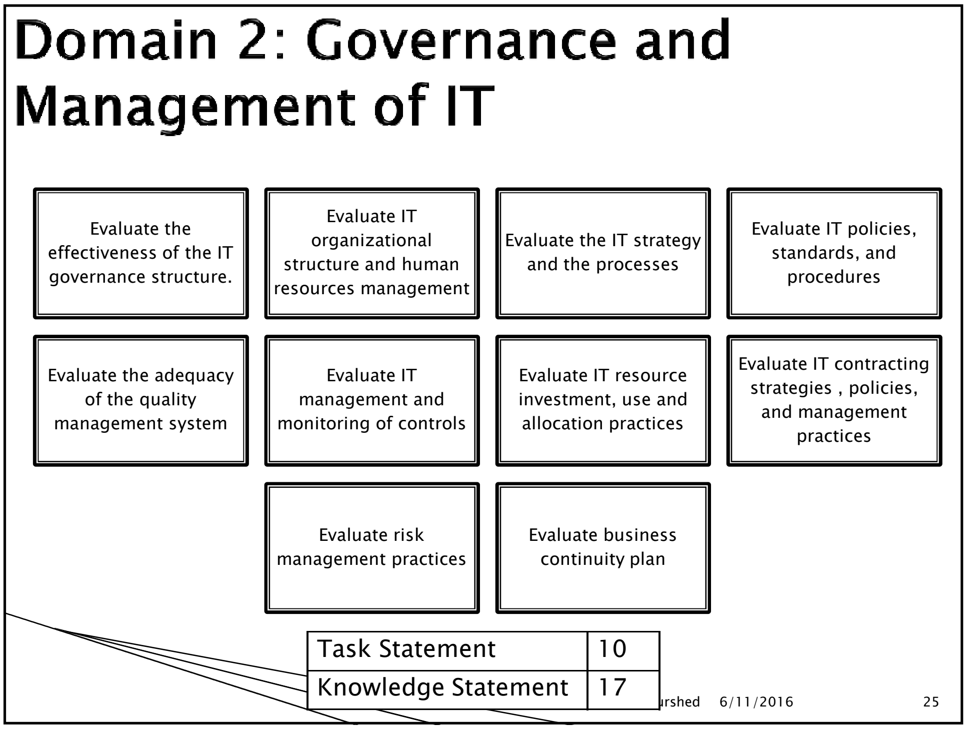
Domain 1: Sample Question

The IS auditor performing a review of an application's control finds a weakness in system software that could materially impact the application

a) Disagree these control weaknesses since a system software review is beyond the scope this review
b) Conduct a detailed system software review and report the control weakness
c) Include in the report a statement that the audit was limited to review of the application controls
d) Review the system software controls as relevant and recommended a detailed system software review



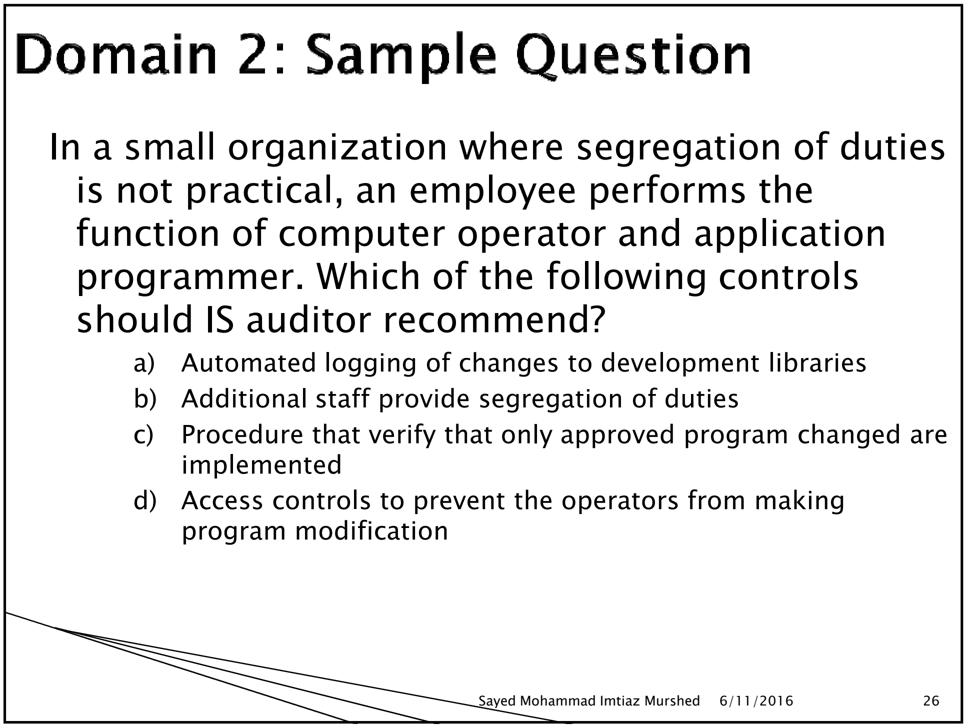
1-5 **D** The IS auditor is not expected to ignore control weaknesses just because they are outside the scope of a current review. Further, the conduct of a detailed systems software review may hamper the audit's schedule and the IS auditor may not be technically competent to do such a review at this time. If there are control weaknesses that have been discovered by the IS auditor, they should be disclosed. By issuing a disclaimer, this responsibility would be waived. Hence, the appropriate option would be to review the systems software as relevant to the review and recommend a detailed systems software review for which additional resources may be recommended.



Domain 2: Governance and Management of IT

- Evaluate the effectiveness of the IT governance structure.
- Evaluate IT organizational structure and human resources management
- Evaluate the IT strategy and the processes
- Evaluate IT policies, standards, and procedures
- Evaluate the adequacy of the quality management system
- Evaluate IT management and monitoring of controls
- Evaluate IT resource investment, use and allocation practices
- Evaluate IT contracting strategies , policies, and management practices
- Evaluate risk management practices
- Evaluate business continuity plan

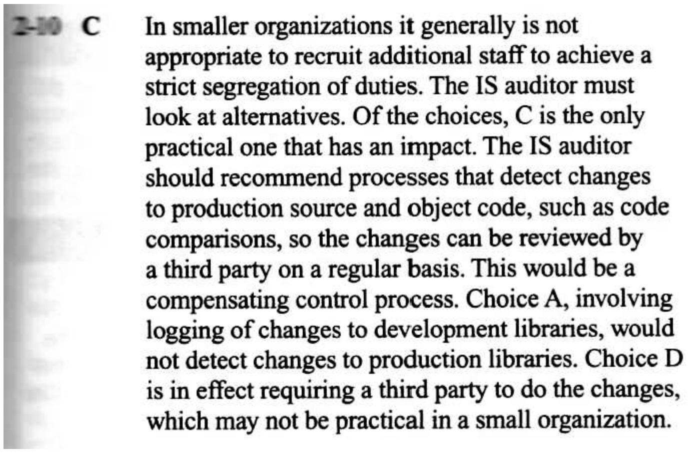
Task Statement	10
Knowledge Statement	17



Domain 2: Sample Question

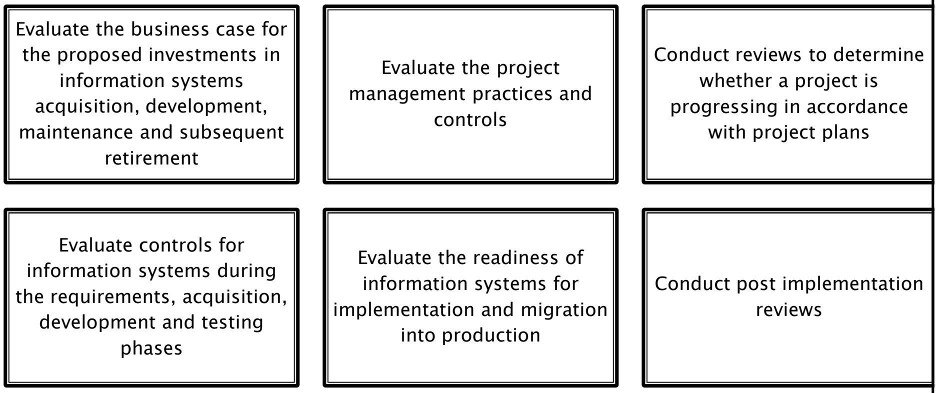
In a small organization where segregation of duties is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should IS auditor recommend?

a) Automated logging of changes to development libraries
b) Additional staff provide segregation of duties
c) Procedure that verify that only approved program changed are implemented
d) Access controls to prevent the operators from making program modification



2-10 C In smaller organizations it generally is not appropriate to recruit additional staff to achieve a strict segregation of duties. The IS auditor must look at alternatives. Of the choices, C is the only practical one that has an impact. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed by a third party on a regular basis. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

Domain 3: IS Acquisition, Development and Implementation



Evaluate the business case for the proposed investments in information systems acquisition, development, maintenance and subsequent retirement

Evaluate the project management practices and controls

Conduct reviews to determine whether a project is progressing in accordance with project plans

Evaluate controls for information systems during the requirements, acquisition, development and testing phases

Evaluate the readiness of information systems for implementation and migration into production

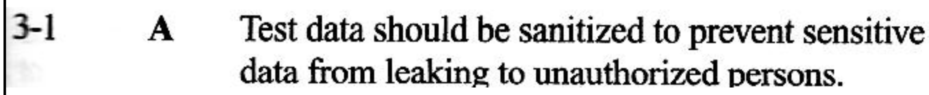
Conduct post implementation reviews

Task Statement	7
Knowledge Statement	14

Domain 3: Sample Question

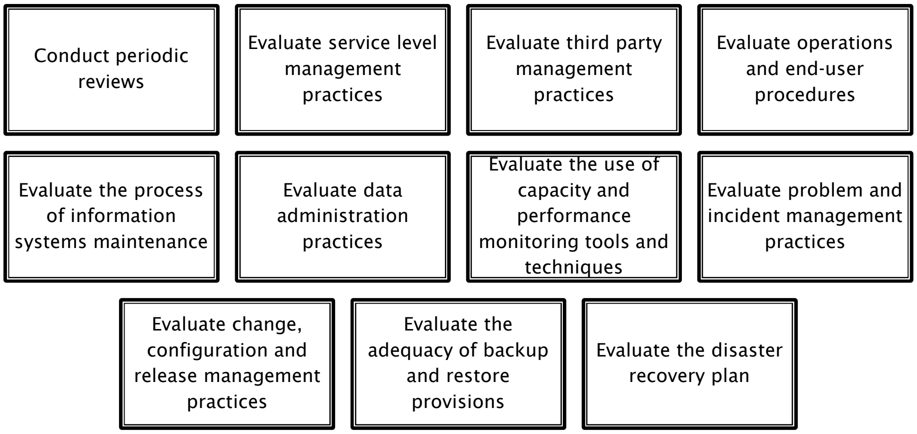
To assist in testing a core banking system being acquired, an organization has provided the vendor with sensitive data from its existing production system. An IS auditor's primary concern is that the data should be

a) Sanitized
b) Complete
c) Representative
d) Current



3-1 A Test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

Domain 4: Information Systems Operations, Maintenance and Support


Conduct periodic reviews
Evaluate service level management practices
Evaluate third party management practices
Evaluate operations and end-user procedures
Evaluate the process of information systems maintenance
Evaluate data administration practices
Evaluate the use of capacity and performance monitoring tools and techniques
Evaluate problem and incident management practices
Evaluate change, configuration and release management practices
Evaluate the adequacy of backup and restore provisions
Evaluate the disaster recovery plan

Task Statement	10
Knowledge Statement	23

Domain 4: Sample Question

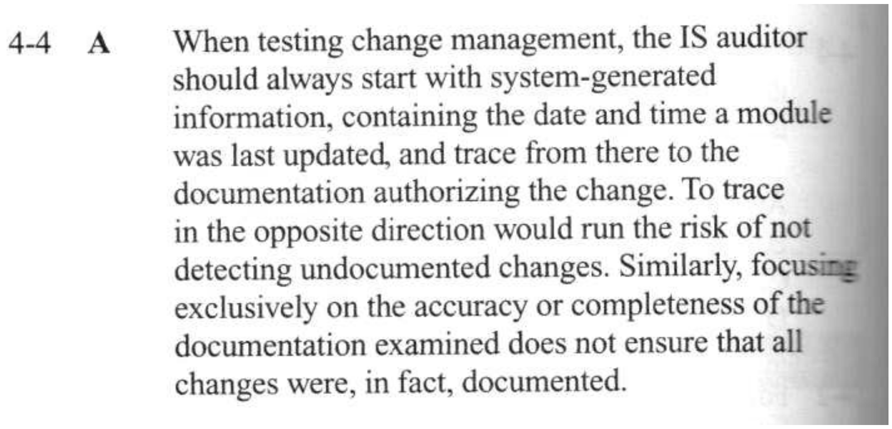
Which of the following is the MOST effective method for an IS auditor to use in testing the program change management process?

A. Trace from system – generated information to the change management documentation

B. Examine change management documents for evidence of accuracy

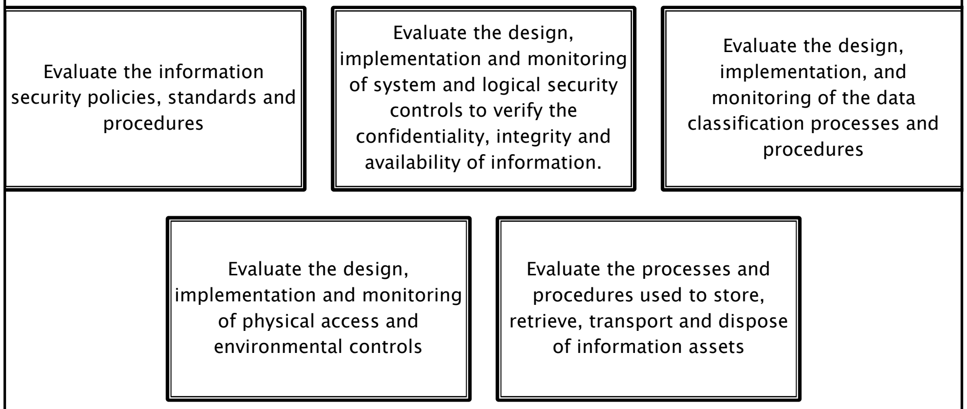
C. Trace from the change management documentation to a system generated audit trial

D. Examine change management documentation for evidence of completeness



4-4 **A** When testing change management, the IS auditor should always start with system-generated information, containing the date and time a module was last updated, and trace from there to the documentation authorizing the change. To trace in the opposite direction would run the risk of not detecting undocumented changes. Similarly, focusing exclusively on the accuracy or completeness of the documentation examined does not ensure that all changes were, in fact, documented.

Domain 5: Protection of Information Assets



Evaluate the information security policies, standards and procedures

Evaluate the design, implementation and monitoring of system and logical security controls to verify the confidentiality, integrity and availability of information.

Evaluate the design, implementation, and monitoring of the data classification processes and procedures

Evaluate the design, implementation and monitoring of physical access and environmental controls

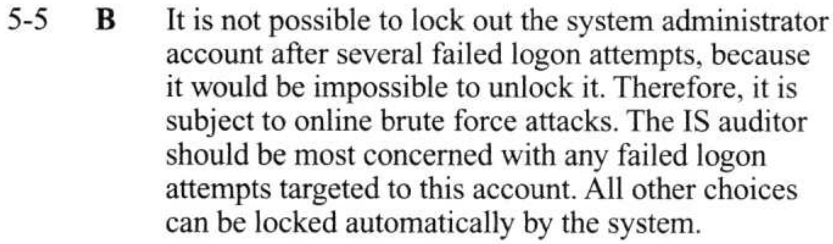
Evaluate the processes and procedures used to store, retrieve, transport and dispose of information assets

Task Statement	6
Knowledge Statement	26

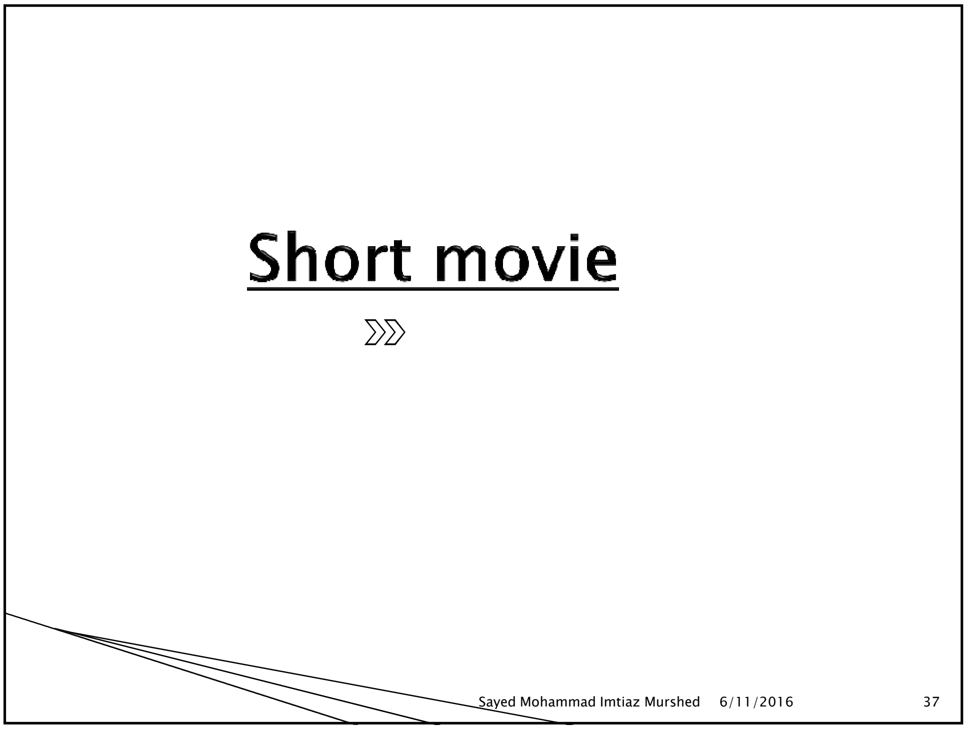
Domain 5: Sample Question

An IS auditor reviewing the log of failed logon attempts would be MOST concerned if which of the following accounts was targeted?

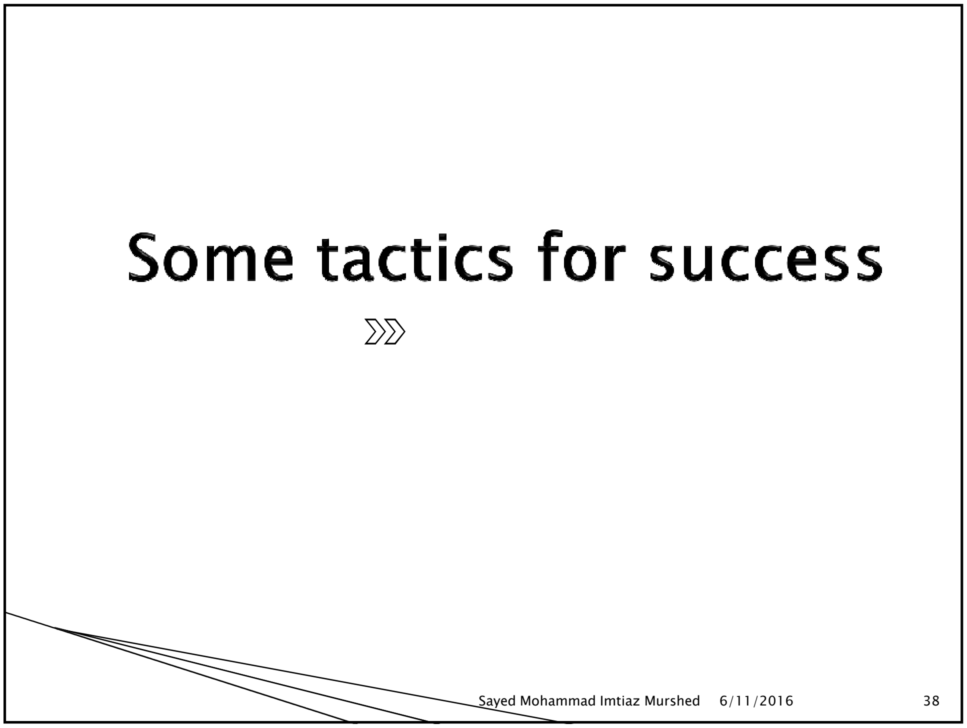
A. Network administrator
B. System administrator
C. Data administrator
D. Database administrator



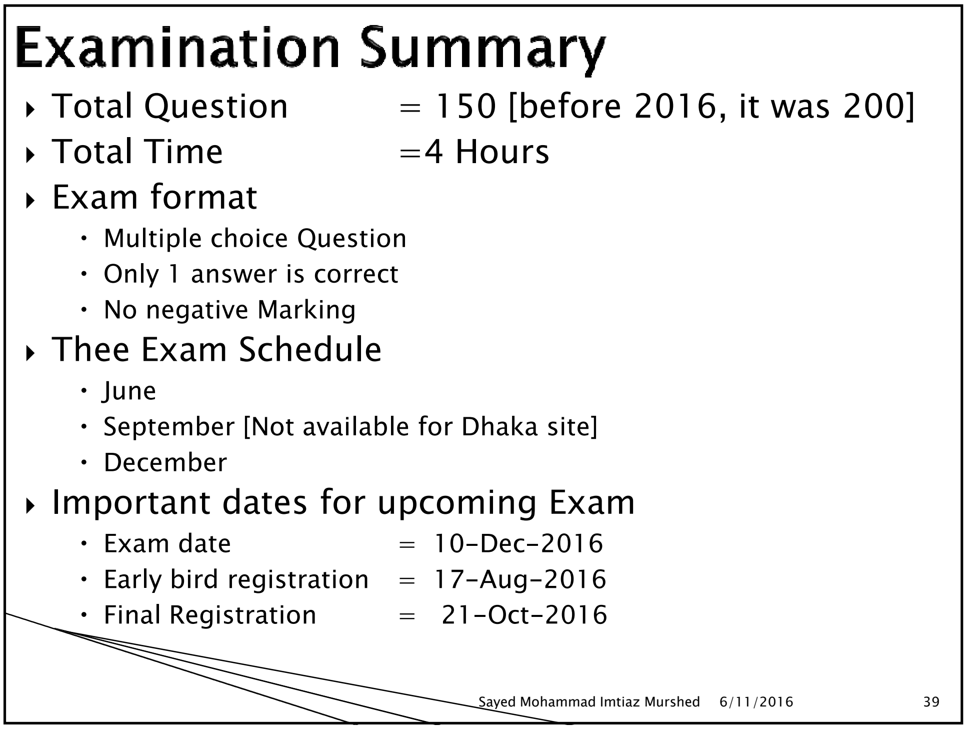
5-5 **B** It is not possible to lock out the system administrator account after several failed logon attempts, because it would be impossible to unlock it. Therefore, it is subject to online brute force attacks. The IS auditor should be most concerned with any failed logon attempts targeted to this account. All other choices can be locked automatically by the system.



Short movie

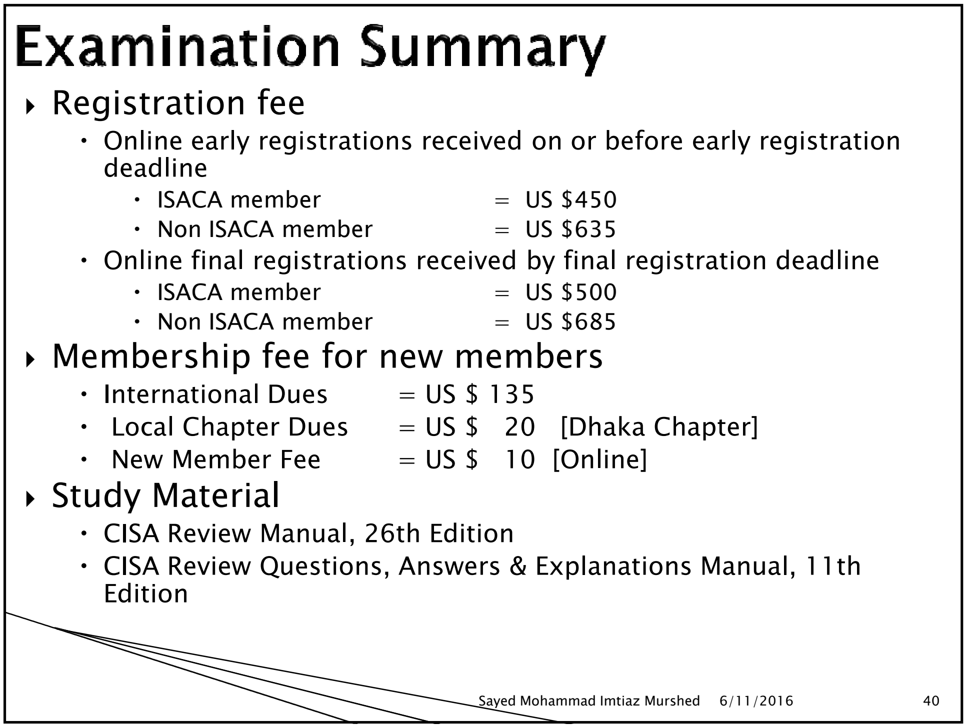


Some tactics for success



Examination Summary

- Total Question = 150 [before 2016, it was 200]
- Total Time =4 Hours
- Exam format
  - Multiple choice Question
  - Only 1 answer is correct
  - No negative Marking
- Thee Exam Schedule
  - June
  - September [Not available for Dhaka site]
  - December
- Important dates for upcoming Exam
  - Exam date = 10-Dec-2016
  - Early bird registration = 17-Aug-2016
  - Final Registration = 21-Oct-2016



Examination Summary

- Registration fee
  - Online early registrations received on or before early registration deadline
    - ISACA member = US $450
    - Non ISACA member = US $635
  - Online final registrations received by final registration deadline
    - ISACA member = US $500
    - Non ISACA member = US $685
- Membership fee for new members
  - International Dues = US $ 135
  - Local Chapter Dues = US $ 20 [Dhaka Chapter]
  - New Member Fee = US $ 10 [Online]
- Study Material
  - CISA Review Manual, 26th Edition
  - CISA Review Questions, Answers & Explanations Manual, 11th Edition

Days Remaining

182

Before Examination Preparation

- Decide early
- Make a time plan
- Motivation is an important aspect
- Don’t stay up late
- Use CISA review Manual
- Understand clearly
- Exam is not technology or platform specific
- Use CISA questions, answer and explanation manual
- Focus on ensuring you get required knowledge
- Form study group
- Practice, practice and practice

Approach to exam

- Think like IT auditor
- Familiarize yourself with the test
- There are 150 questions to be answered in four hour
- Remember that CISA is an objective type exam
- Learn to play the game of CISA

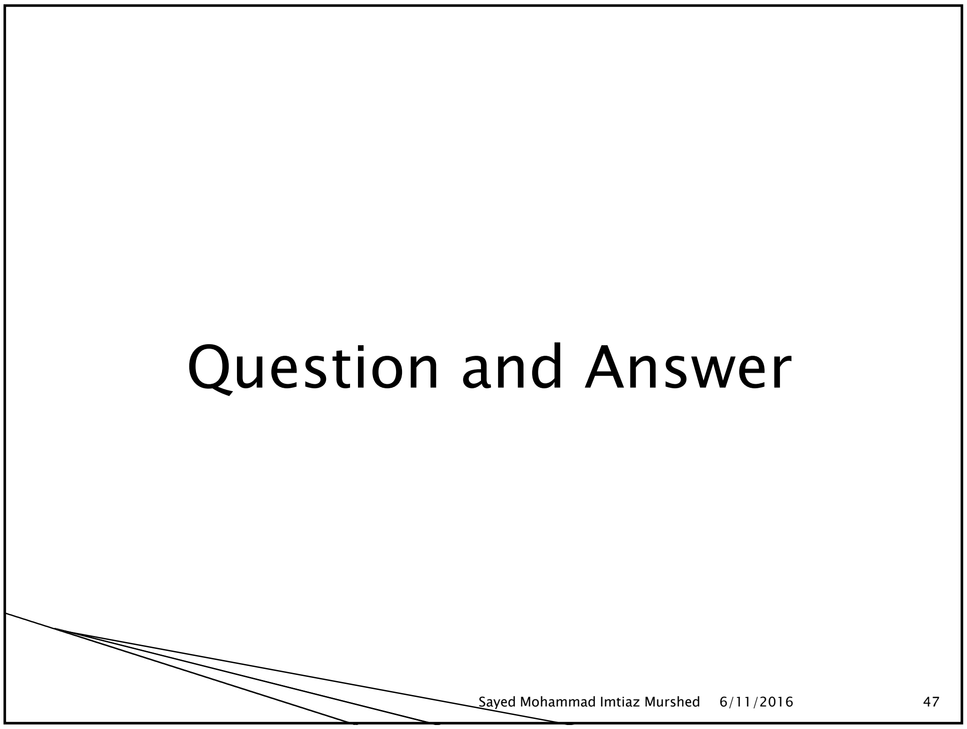
Manage your exam time

Per question **96** seconds

During Examination

- Don’t attempt to read through the question paper fully
- Take one question at a time
- Read question carefully
- Don’t think to come back
- No negative marking
- Choose the right answer
- Concentration level
- You may encounter some questions which are familiar to you

Thank you



Question and Answer